

1 **CLAIMS**

2

3 1. A programming interface embodied on one or more computer

4 readable media, comprising:

5 a first group of functions related to communicating a new security policy to

6 a plurality of security engines, wherein each of the plurality of security engines is

7 configured to replace an existing security policy with the new security policy; and

8 a second group of functions related to communicating an indication of each

9 security engine's readiness to implement the new security policy.

10

11 2. A programming interface as recited in claim 1 wherein the first group

12 of functions includes a method that instructs each of the plurality of security

13 engines to delete the new security policy.

14

15 3. A programming interface as recited in claim 1 wherein the first group

16 of functions includes a method that initializes a particular security engine.

17

18 4. A programming interface as recited in claim 1 wherein the first group

19 of functions includes a method that instructs each of the plurality of security

20 engines to implement the new security policy.

21

22 5. A programming interface as recited in claim 1 wherein the first group

23 of functions further comprises a method that communicates new data associated

24 with an existing security policy to at least one of the plurality of security engines.

25

1           6.    A programming interface as recited in claim 1 wherein the first group  
2 of functions further comprises a method that communicates configuration  
3 information to at least one of the plurality of security engines.  
4

5           7.    A programming interface as recited in claim 1 wherein the second  
6 group of functions includes a method that indicates whether a particular security  
7 engine has implemented the new security policy.  
8

9           8.    A programming interface as recited in claim 1 wherein the second  
10 group of functions further comprises a method that retrieves updated data  
11 associated with a particular security policy.  
12

13          9.    A programming interface as recited in claim 1 wherein the second  
14 group of functions further comprises a method that communicates new data  
15 identified by one of the plurality of security engines to a security agent.  
16

17          10.   A programming interface as recited in claim 1 wherein the second  
18 group of functions further comprises a method that allows one of the plurality of  
19 security engines to query a user of a system containing the plurality of security  
20 engines.  
21

22          11.   A programming interface as recited in claim 1 wherein at least one  
23 of the plurality of security engines implements an antivirus service.  
24  
25

1           **12.**    A programming interface as recited in claim 1 wherein at least one  
2 of the plurality of security engines implements a firewall application.

3  
4           **13.**    A programming interface as recited in claim 1 wherein the plurality  
5 of security engines implement the new security policy after all security engines  
6 have indicated a readiness to implement the new security policy.

7  
8           **14.**    A computer system including one or more microprocessors and one  
9 or more software programs, the one or more software programs utilizing an  
10 application program interface to implement a security policy on a plurality of  
11 security engines, the application program interface comprising the following  
12 functions:

13               a first function that communicates a new security policy to the plurality of  
14 security engines;

15               a second function that identifies whether each of the plurality of security  
16 engines is prepared to apply the new security policy; and

17               a third function that instructs each of the plurality of security engines to  
18 implement the new security policy after determining that all of the security  
19 engines are prepared to apply the new security policy.

20  
21           **15.**    A computer system as recited in claim 14 further comprising a  
22 fourth function that causes each of the plurality of security engines to delete the  
23 new security policy if at least one of the plurality of security engines is unable to  
24 apply the new security policy.

1           **16.**    A computer system as recited in claim 14 further comprising a  
2 fourth function related to communicating event information identified by a first  
3 security engine to the other security engines.

4  
5           **17.**    A computer system as recited in claim 14 further comprising a  
6 fourth function related to communicating security-related information identified  
7 by a first security engine to an event manager.

8  
9           **18.**    A computer system as recited in claim 17 wherein the event  
10 manager communicates the security-related information to at least one of the  
11 plurality of security engines.

12  
13           **19.**    A computer system as recited in claim 14 wherein at least one of the  
14 plurality of security engines is associated with a first type of security attack.

15  
16           **20.**    A computer system as recited in claim 19 wherein at least one of the  
17 plurality of security engines is associated with a second type of security attack.

18  
19           **21.**    A method comprising:  
20           calling one or more first functions to facilitate communicating a security  
21 policy to a first security engine;  
22           calling one or more second functions to facilitate determining whether the  
23 first security engine has applied the security policy; and  
24           calling one or more third functions to facilitate communicating security-  
25 related information from the first security engine to a second security engine.

1  
2       **22.**    A method as recited in claim 21 wherein the security-related  
3 information identifies a type of security attack.  
4

5       **23.**    A method as recited in claim 21 further comprising calling one or  
6 more fourth functions to facilitate interacting with a user of a system containing  
7 the first security engine.  
8

9       **24.**    A method as recited in claim 21 further comprising calling one or  
10 more fourth functions to facilitate communicating configuration information to the  
11 first security engine.  
12

13       **25.**    A method as recited in claim 21 further comprising calling one or  
14 more fourth functions to facilitate instructing the first security engine and the  
15 second security engine to implement the security policy.  
16

17       **26.**    A method as recited in claim 21 further comprising calling one or  
18 more fourth functions to facilitate communicating a revised security policy to the  
19 first security engine.  
20

21       **27.**    A system comprising:  
22       means for exposing a first function that communicates a security-related  
23 event to an event manager;  
24       means for exposing a second function that identifies a plurality of security  
25 engines associated with the security-related event; and

1 means for exposing a third function that communicates the security-related  
2 event to the identified security engines.

3  
4 **28.** A system as recited in claim 27 further comprising:  
5 means for exposing a fourth function that communicates a new security  
6 policy to the plurality of security engines; and  
7 means for exposing a fifth function that instructs the plurality of security  
8 engines to replace an existing security policy with the new security policy.

9  
10 **29.** A system as recited in claim 28 further comprising means for  
11 exposing a sixth function that instructs the plurality to security engines to delete  
12 the new security policy if at least one of the plurality of security engines cannot  
13 implement the new security policy.

14  
15 **30.** A system as recited in claim 27 wherein the security-related event is  
16 detection of a virus.

17  
18 **31.** A system as recited in claim 27 wherein the security-related event is  
19 an unauthorized attempt to access a storage device.

20  
21 **32.** A system as recited in claim 27 further comprising means for  
22 exposing a fourth function that notifies the event manager that a particular security  
23 engine has finished processing another function call.